A
PROJECT PHASE-I REPORT
ON

Vulnerable University

SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE

OF

BACHELOR OF TECHNOLOGY (COMPUTER ENGINEERING)

SUBMITTED BY

Abhishek Birdawade – BCOA03
Srushti Deshpande – BCOB93
Vaibhav Wagh – BCOB111

Under the Guidance of
Ms. Gayatri Bedre

DEPARTMENT OF COMPUTER ENGINEERING

G. H. RAISONI COLLEGE OF ENGINEERING AND MANAGEMENT
(An Autonomous Institute affiliated to SPPU)
WAGHOLI, PUNE-402207

SAVITRIBAI PHULE PUNE UNIVERSITY
2022 -2023

G. H. Raisoni College of Engineering and Management, Wagholi- Pune 402207

(An Autonomous Institute affiliated to SPPU)

CERTIFICATE

This is to certify that the project report entitles
“Vulnerable University”

Submitted by

Abhishek Birdawade	**Exam No: BCOA03**
Srushti Deshpande	**Exam No: BCOB93**
Vaibhav Wagh	**Exam No: BCOB111**

are bonafide students at this institute and the work has been carried out by them under the supervision of **Ms. Gayatri Bedre** and it is approved for the partial fulfillment of the requirement of Savitribai Phule Pune University, for the award of the degree of **Bachelor of Technology** (Computer Engineering).

Ms. Gayatri Bedre
Guide
Department of Computer
Engineering

Dr. Simran Khiani
HoD
Department of Computer
Engineering

Dr. R. D. Kharadkar
Director
GHRCEM

Place:

Date:

ACKNOWLEDGEMENT

The satisfaction that accompanies that the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success.

I would like to express deepest appreciation towards Director of G. H. Raisoni college of Engineering and Management, Pune and **Dr. Simran khaini** Head of Department, Computer Engineering whose invaluable guidance supported us in this project.

We are grateful to our project guide **Ms. Gayatri Bedre** for the guidance, inspiration and constructive suggestions that helpful us in the preparation of this project.

Sr. No.	**Name of Student**	**Signature**
1.	Abhishek Birdawade	
2.	Srushti Deshpande	
3.	Vaibhav Wagh	

ABSTRACT

A frequently used method to assess and enhance the security of software is security testing, which identifies vulnerabilities and ensures security functionality. Applying suitable security testing approaches is becoming increasingly important and necessary due to the openness of contemporary software-based systems in order to carry out effective and efficient security testing. Consequently, a summary of current security testing methods is very important for practitioners to use and spread the approaches as well as for researchers to assess and improve the procedures.

It begins by summarizing the necessary background for testing and security engineering for this goal. Then, fundamentals and current research in security testing methods used in the safe software development lifecycle, including model-based security testing, code-based testing and static analysis, penetration testing and dynamic analysis, as well as security.

The field of cyber security is wide and expanding regularly. We need security practitioners and testers to help us combat the growing issue of digital theft and cybercriminals. They must learn how to test without breaking the Cyber law. The dangerous website application will offer a venue where they may practice and test their knowledge in their local System.

TABLE OF CONTENTS

LIST OF ABBREVATIONS

ABBREVIATION	ILLUSTRATION
SQL	Structured Query Language
API	Application Programming Interface
SSRF	Server-Side Request Forgery
XML	Extensible Markup Language

LIST OF FIGURES

CHAPTER – 1
INTRODUCTION

1.1 Motivation –

Cyber Security is method of protecting and securing the computer devices, network and program from cyber-attack. The importance of cyber security is rising. Cyber criminals are more sophisticated, changing the attacking approach and they are creating a really crucial conditions for organizations by affecting their image. An application vulnerability means lack of security or weakness in an application that cause a major issue. This happens due to not validating inputs, flaws in application design and misconfigured servers. Cyber security is a vast field and immerging daily. With increasing digital theft and cyber criminals, we need security tester and practioners to help us tackle the increasing problem. It is necessary for them to learn testing without violating cyber laws. The vulnerable web application will provide a platform to learn and test their skills in their own local environment.

The vulnerable web applications can be used by web developers, security auditors, and penetration testers to practice their knowledge and skills during training sessions (and especially afterwards), as well as to test at any time the multiple hacking tools and offensive techniques out there, in preparation for their next real-world engagement. Intentionally Vulnerable web-applications for testing can help security professionals for hacking, offensive and defensive activities on their local system mimicking realistic web environments. Security professionals can practice and enhance their skills regarding web-application security testing by learning and practicing about various technical and non-technical bugs and vulnerabilities.

1.2 Problem Statement –

The field of cyber security is wide and expanding regularly. We need security practitioners and testers to help us combat the growing issue of digital theft and cybercriminals. They must learn how to test without breaking the Cyber laws. The dangerous website application will offer a venue where they may practice and test their knowledge in their local System.

CHAPTER – 2

LITERATURE SURVEY

Sr. No	Date	Author	Title	Summary
1.	03/11/2015	Michael Felderer, Matthias Büchler, Martin Johns	Security Testing: A Survey	This chapter provided a broad overview of recent security testing techniques
2.	10/03/2016	Min Wei, Shuaidong Zhang, Keecheon Kim	A security testing platform for Wireless Sensor Networks	The test results show that the platform is a feasible platform for assessing device security levels in WSNs.
3.	23/10/2021	Andrew Hahn, Daniel R. Sandoval, Raymond E. Fasano, Christopher Lamb	Automated Cyber Security Testing Platform for Industrial Control System.	A platform that incorporates these three components to provide the most accurate representation of actual NPP networks and controllers is developed in this paper
4.	29/01/2021	Hermawan Setiawan, Lytio Enggar Erlangga, Ido Baskoro	Vulnerability Analysis Using the Interactive Application Security Testing (IAST) Approach for	Using the IAST approach, a total of 249 vulnerability risks were identified.

			Government X Website Applications.	
5.	03/11/2021	Anushka Lal, Girish Kumar	Intelligent Testing in Software Industry	This study aims to investigate the approach of intelligent testing for improving software testability.

CHAPTER – 3
SOFTWARE REQUIREMENTS SPECIFICATIONS

3.1 Introduction –

3.1.1 – Project Scope – Cyber security is a vast field and immerging daily. With increasing digital theft and cyber criminals, we need security tester and practitioner to help us tackle the increasing problem. It is necessary for them to learn testing without violating cyber laws. The vulnerable web application will provide a platform to learn and test their skills in their own local environment.

Currently we are using two technologies i.e., NodeJS & Django but in future we are going to build this platform using almost every framework. So, this is the one of the best platforms where they can have a various bugs using various technologies.

3.2 System Requirements –

3.2.1 – Database Requirements –

- MongoDB
- NoSQL
- JSON
- API’s
- Docker Image
- Docker Container

3.2.2 – Hardware Requirements –

- 1 TB HDD
- 4/8 GB RAM
- i5 or above processor

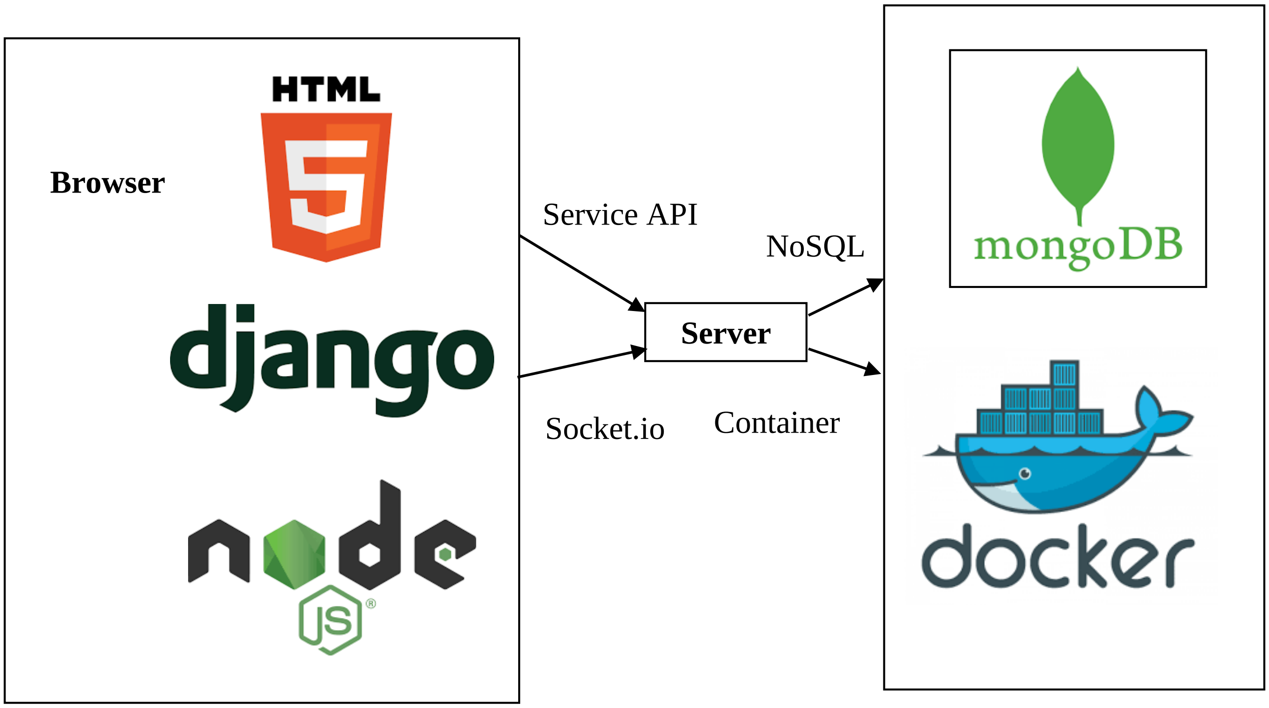
3.2.3 – Software Requirements

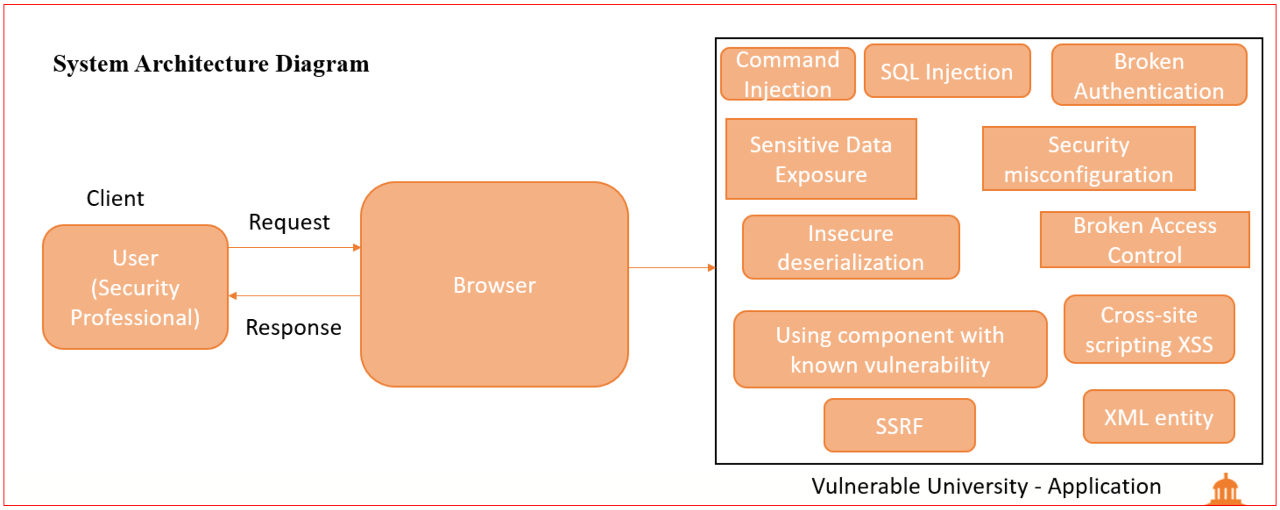
- Operating System – Linux, Windows, Mac
- Web Browser – Chrome, Firefox, etc

CHAPTER – 4

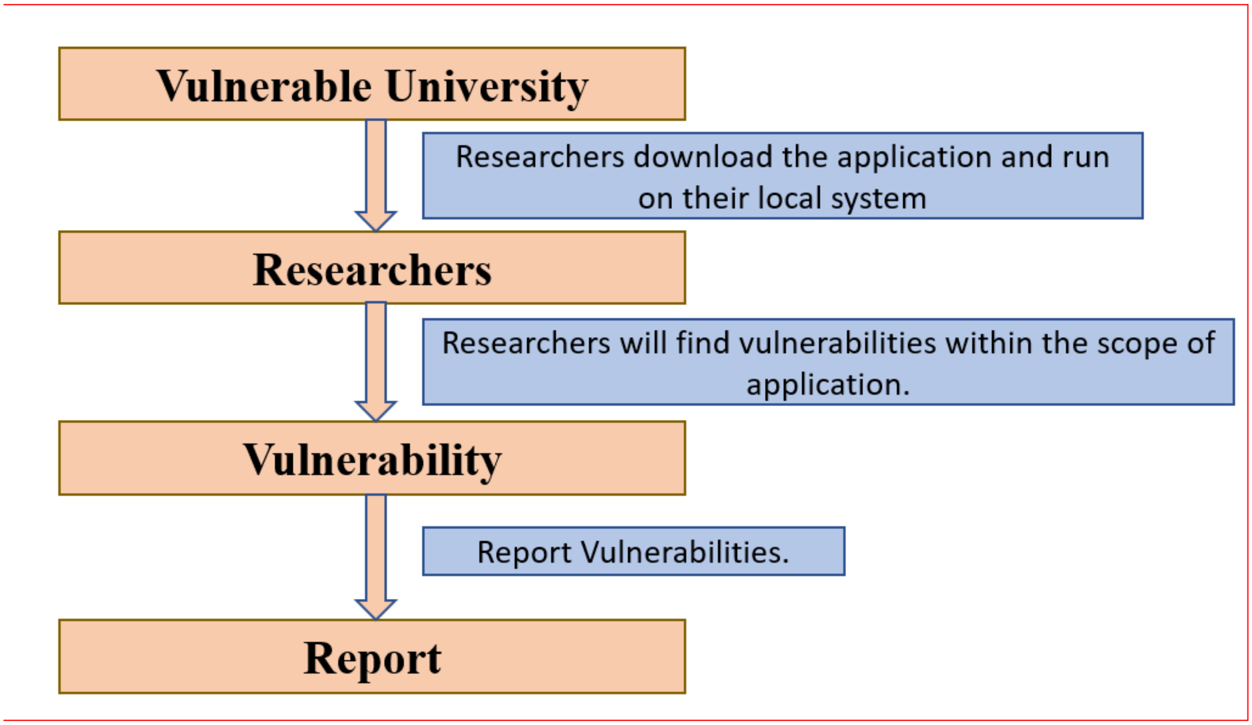
SYSTEM DESIGN

4.1 System Architecture –

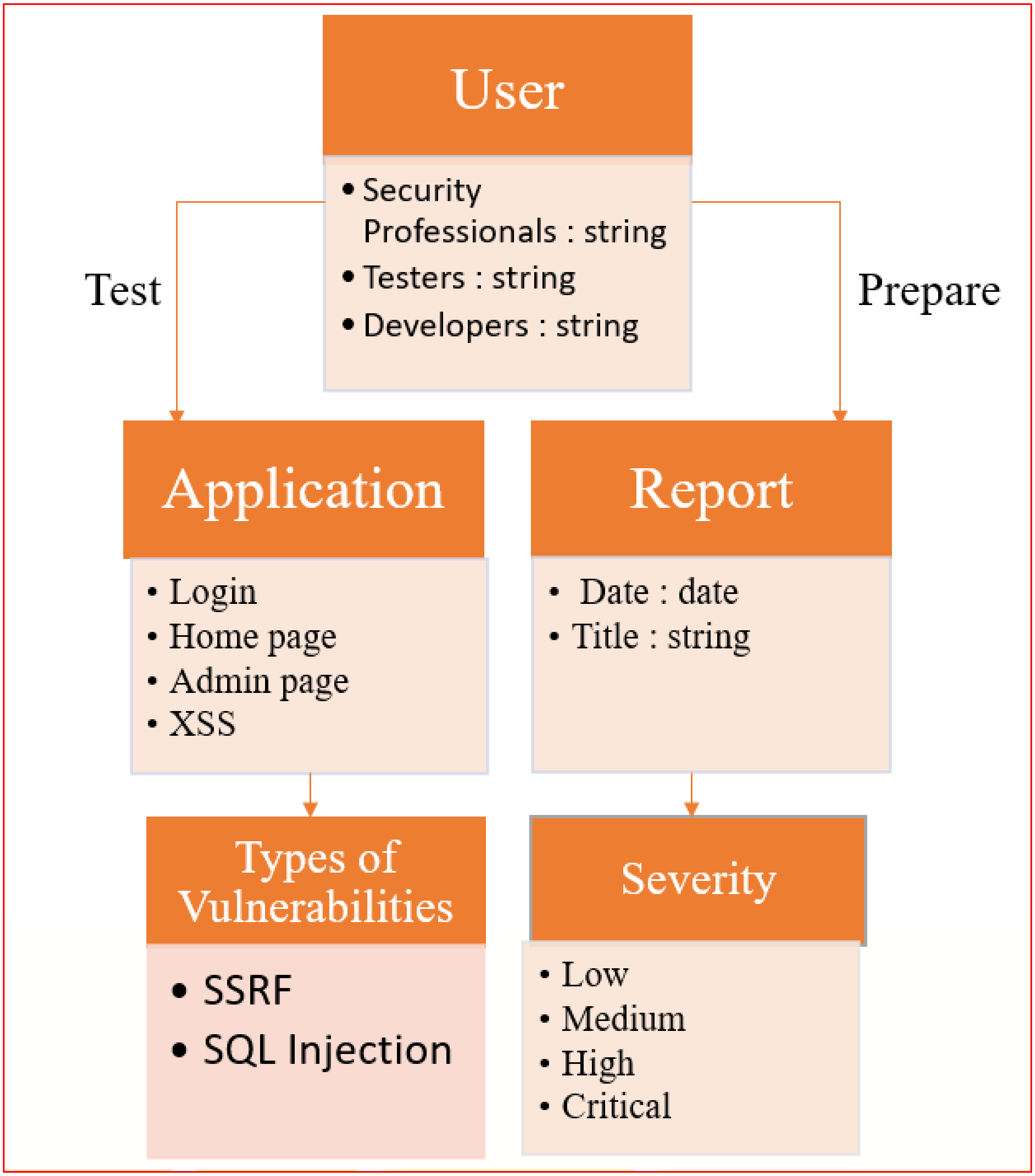




4.2 Block Diagram –


Vulnerable University
Researchers download the application and run on their local system
Researchers
Researchers will find vulnerabilities within the scope of application.
Vulnerability
Report Vulnerabilities.
Report

4.3 UML Diagram –



CHAPTER – 5
OTHER SPECIFICATIONS

5.1 Advantages –

- Vulnerable University is a platform, which have various kind of vulnerabilities there to practice.
- This application is free to for anyone and easily available for them.
- It is platform independent.
- This application is not only for testing or practicing but also for learning different types of bugs.
- Security Professionals and students can have various types of bugs in different technologies on a single platform.

5.2 Applications –

- Security Professionals can brush up their skills regularly.
- Students can learn, ethical hacking on that platform.
- They will learn that how to make valid reports.
- Developers can learn, how to do secure coding.

CHAPTER – 6
CONCLUSION

Cyber security is the method of protecting computer devices, networks and programs from cyberattacks. Cyber security is becoming more and more important. cybercriminals are becoming more sophisticated, changing their attack methods and damaging an organization’s image, creating very important conditions for an organization.

Vulnerable University helps improve the skills of security professionals and this application helps raise awareness of ethical hacking among students. Anyone can easily access this free application and run it locally. Students can learn the necessary skills and earn a good amount of money by finding bugs that work for many organizations on various platforms.

CHAPTER – 7
REFERENCES

[1] Adam Doupe and Marco Cova and Giovanni Vigna. Why johnny can't pentest: An analysis of black-box web vulnerability scanners. In DIMVA 2010, 2010.

[2] N. Ayewah, D. Hovemeyer, J. D. Morgenthaler, J. Penix, and W. Pugh. Experiences using static analysis to find bugs. IEEE Software, 25:22– 29, 2008. Special issue on software development tools, September/October (25:5).

[3] R. Bachmann and A. D. Brucker. Developing secure software: A holistic approach to security testing. Datenschutz und Datensicherheit (DuD), 38(4):257–261, apr 2014.

[4] R. Bachmann and A. D. Brucker. Developing secure software: A holistic approach to security testing. Datenschutz und Datensicherheit (DuD), 38(4):257–261, apr 2014.

[5] P. Ammann and J. Offutt. Introduction to Software Testing. Cambridge University Press, Cambridge, UK, 2008.

[6] J. Grossman, R. Hansen, P. Petkov, and A. Rager. Cross Site Scripting Attacks: XSS Exploits and Defense. Syngress, 2007.

[7] M. Anisetti, C. Ardagna, and E. Damiani. A low-cost security certification scheme for evolving services. In Web Services (ICWS), 2012 IEEE 19th International Conference on, pages 122–129, June 2012.

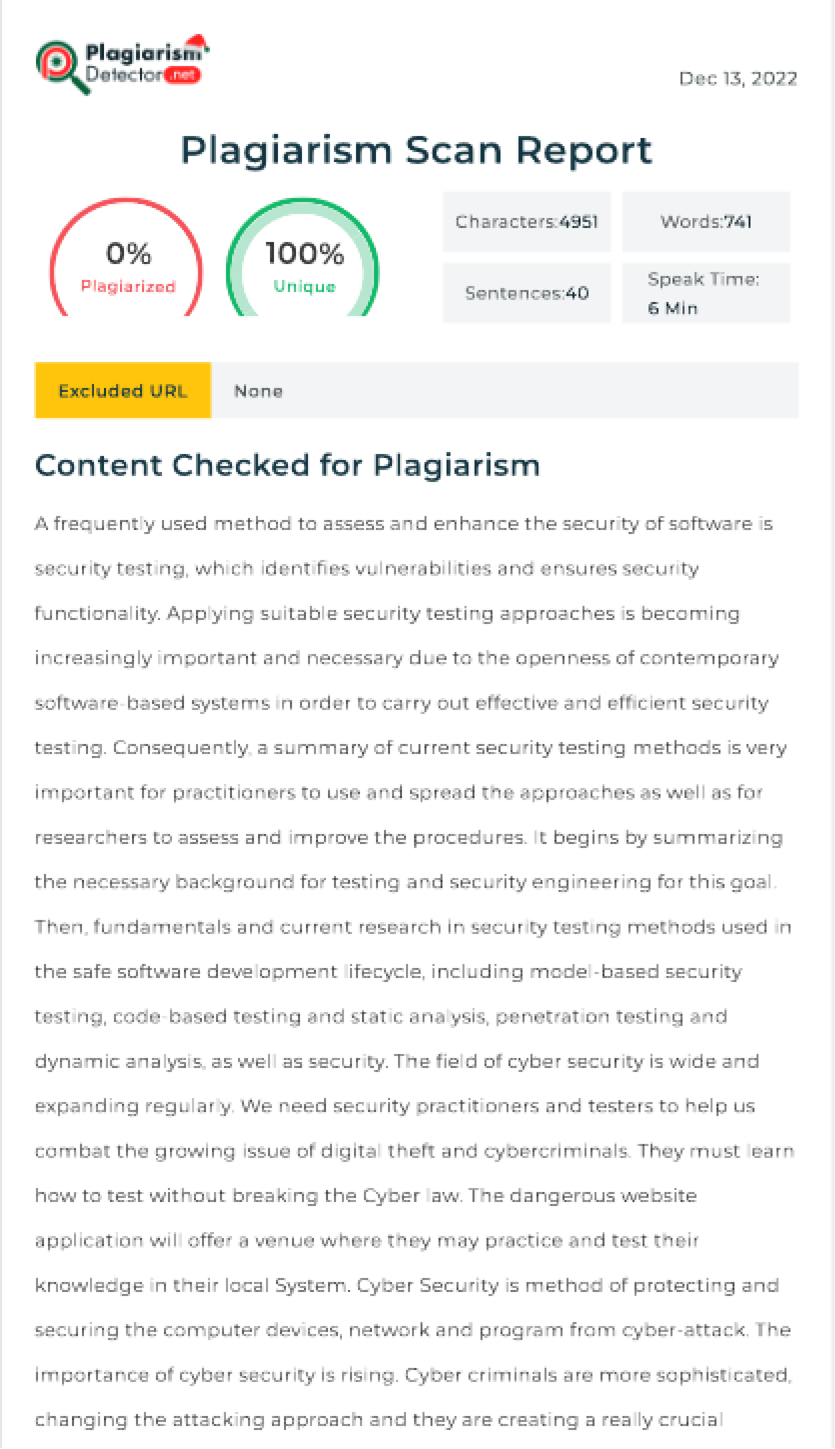
[8] B. Arkin, S. Stender, and G. McGraw. Software penetration testing. Security & Privacy, IEEE, 3(1):84–87, 2005.

[9] Bau, E. Bursztein, D. Gupta, and J. Mitchell. State of the art: Automated black-box web application vulnerability testing. In Security and Privacy (SP), 2010 IEEE Symposium on, pages 332–345. IEEE, 2010.

[10] D. Brucker, L. Br¨ugger, and B. Wolff. Formal firewall conformance testing: An application of test and proof techniques. Software Testing, Verification & Reliability (STVR), 25(1):34–71, 2015.

[11] Zander, I. Schieferdecker, and P. J. Mosterman. Model-based testing for embedded systems, volume 13. CRC Press, 2012.

APPENDIX – A



Plagiarism Detector.net

Dec 13, 2022

Plagiarism Scan Report

0% Plagiarized

100% Unique

Characters:4951	Words:741
Sentences:40	Speak Time: 6 Min

Excluded URL	None

Content Checked for Plagiarism

A frequently used method to assess and enhance the security of software is security testing, which identifies vulnerabilities and ensures security functionality. Applying suitable security testing approaches is becoming increasingly important and necessary due to the openness of contemporary software-based systems in order to carry out effective and efficient security testing. Consequently, a summary of current security testing methods is very important for practitioners to use and spread the approaches as well as for researchers to assess and improve the procedures. It begins by summarizing the necessary background for testing and security engineering for this goal. Then, fundamentals and current research in security testing methods used in the safe software development lifecycle, including model-based security testing, code-based testing and static analysis, penetration testing and dynamic analysis, as well as security. The field of cyber security is wide and expanding regularly. We need security practitioners and testers to help us combat the growing issue of digital theft and cybercriminals. They must learn how to test without breaking the Cyber law. The dangerous website application will offer a venue where they may practice and test their knowledge in their local System. Cyber Security is method of protecting and securing the computer devices, network and program from cyber-attack. The importance of cyber security is rising. Cyber criminals are more sophisticated, changing the attacking approach and they are creating a really crucial